



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/734,184	12/15/2003	Yuuki Miyazaki	25880	2153

20529 7590 09/28/2007  
NATH & ASSOCIATES  
112 South West Street  
Alexandria, VA 22314

EXAMINER
----------

ZEE, EDWARD

ART UNIT	PAPER NUMBER
----------	--------------

2135

MAIL DATE	DELIVERY MODE
-----------	---------------

09/28/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

## Office Action Summary

Application No.

10/734,184

Applicant(s)

MIYAZAKI, YUUKI

Examiner

Edward Zee

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 29 June 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 7-9 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 7-9 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 29 June 2007 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- ☐ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date 8/30/07.
- ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- ☐ Notice of Informal Patent Application
- ☐ Other: \_\_\_\_\_.

### **DETAILED ACTION**

1. This is in response to the amendment filed on June 29<sup>th</sup>, 2007. Claims 1-6 have been cancelled, Claims 7-9 have been added and Claims 7-9 are pending and have been considered below.

#### ***Drawings***

2. The replacement drawings were received on June 29<sup>th</sup>, 2007. Therefore the previous objections to the drawings are withdrawn.

#### ***Specification***

3. The amendments submitted on June 29<sup>th</sup>, 2007 effectively overcome the previous objections. Therefore, the objections to the specification are withdrawn.

#### ***Claim Rejections - 35 USC § 112***

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claim 7 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Art Unit: 2135

Claim 7 discloses, in lines 19-20 of the claim, performing a determination step on the “terminal code”, which in particular requires determining if a “terminal code” is equal to or less than a predetermined number. This newly claimed feature does not appear to be supported by the original specification. The Examiner notes that the original specification discloses, on page 18 lines 16-17, a determination step, which includes the step of determining whether the *number of records* having a matching license code and a different MAC address *is two or less*.

6. Claim 7 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

Claim 7 discloses, in lines 19-20 of the claim, performing a determination step on the “terminal code”, which in particular requires determining if a “terminal code” is equal to or less than a predetermined number, and based on this determination, continuing the process of releasing the functional limitation of the software if the code is less than or equal to the predetermined number, or alternatively, exiting the process of releasing the software if the code is greater than the number.

The Applicant appears to submit that the “terminal code” corresponds to a MAC address of a user terminal as disclosed in the specification. However, the Examiner notes that a MAC address consists of a complex string of data comprising letters and numbers(ie. 00-80-88-41-11-a2), as can be seen in Figure 2 of the Applicant’s own disclosure.

The Examiner notes that one of ordinary skill in the art would not know how to perform a comparison of two MAC addresses and determine which one is the lesser of the two, nor would

Art Unit: 2135

one be able to compare a MAC address to a predetermined number and conclude if it is equal to or less than the number.

Therefore, this feature will be interpreted as continuing the software releasing process if the terminal code is equal to a predetermined terminal code, and exiting the process if it is not equal.

***Claim Rejections - 35 USC § 103***

7. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

8. **Claims 7-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sprong et al. (6,134,659) in view of Hicks et al. (5,982,892), in further view of Hillier et al. (6,055,636).**

***Claim 7:*** Sprong et al. discloses a license management method and system comprising:

- a. attaching an identification code(*identification number*) to the software product [column 9, lines 44-46];
- b. sending identification code(*identification number*) and terminal code(*serial number*) to authentication server(*remote authorization unit*) [column 10, lines 19-23];
- c. a recording step, by said authentication server(*remote authorization unit*), of comparing the identification code and the terminal code with the license information recorded in the database and, if a predetermined condition is satisfied, recording(*collecting*) the identification code and the terminal code in the database [column 10, lines 23-30];

Art Unit: 2135

d. a digital signature step, by said authentication server, signing the identification code and the terminal code into an authorization code(*authorization code algorithm*) [column 10, lines 30-41];

e. a checking step, by said user terminal, of checking validity of the authorization code received from the authorization server(*remote authorization unit*) [column 10, lines 49-51];

f. and a limitation release step, by said user terminal, of releasing a functional limitation of the software(*enabling the use of the software*) based on the checking result of said checking step [column 10, lines 60-66].

However, Sprong et al. does not explicitly disclose:

a. a first digital signature creation step of creating, by said product management server, a first digital signature from the identification code using a private key of said product management server, said first digital signature being attached to the software product;

b. a second digital signature creation step, by said route server, of obtaining a public key of said product management server from said product management server and creating a second digital signature from the public key of said product management server using a private key of said route server;

c. a third digital signature creation step, by said route server, of obtaining a public key of said authentication server from said authentication server and creating a third digital signature from the public key of said authentication server using the private key of said route server;

d. a first checking step, by said authentication server, of checking validity of the second digital signature using the public key of said route server obtained from said route server and, based on the checking result, obtaining the public key of said product management server;

e. a second checking step, by said authentication server, of checking validity of the first digital signature using the public key of said product management server in response to the first digital signature and the terminal code from said user terminal and, based on the checking result, obtaining the identification code;

f. a third checking step, by said user terminal, of checking validity of the third digital signature using the public key of said route server obtained from said route server and, based on the checking result, obtaining the public key of said authentication server.

g. a fourth checking step, by said user terminal, of checking validity of the fourth digital signature using the public key of said authentication server obtained in said third checking step and, based on the checking result, obtaining the identification code and the terminal code;

Nonetheless, Hicks et al. discloses a similar license management method and system and further discloses:

a. a digital signature creation step of creating, by a product management server(*product key generator*), a digital signature from the identification code using a private key of said product management server, said digital signature being attached to the software product [column 1, lines 46-51 and column 6, lines 42-47];

b. a checking step, by a user key verifier, of checking validity of the first digital signature using the public key of said product management server(*product key generator*) in response to the first digital signature from said user terminal and, based on the checking result, obtaining the identification code(*product-identifying information*) [column 8, lines 46-56 and column 6, lines 42-47];

c. a fourth digital signature creation step, by said authentication server(*user key generator*), of creating a fourth digital signature from the identification information using a private key(*random or pseudorandom integer*) of said authentication server [column 7, 7-10]. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to digitally sign the identification code and confirm the validity of the signature at the authentication server disclosed by Sprong et al. using the private key of the product management server; and also use public key cryptography when digitally signing the identification code and terminal code of the authentication server. One would have been motivated to do so in order to increase the security and further prevent tampering by using a proven form of cryptography. Though, neither explicitly discloses:

a. a second digital signature creation step, by said route server, of obtaining a public key of said product management server from said product management server and creating a second digital signature from the public key of said product management server using a private key of said route server;

b. a third digital signature creation step, by said route server, of obtaining a public key of said authentication server from said authentication server and creating a third digital signature from the public key of said authentication server using the private key of said route server;

c. a first checking step, by said authentication server, of checking validity of the second digital signature using the public key of said route server obtained from said route server and, based on the checking result, obtaining the public key of said product management server;



d. a third checking step, by said user terminal, of checking validity of the third digital signature using the public key of said route server obtained from said route server and, based on the checking result, obtaining the public key of said authentication server.

The examiner notes that it is old and well known in the cryptographic art to further digitally sign a signature public key with a private key of a certificate authority {route server} and to use the trusted public key of the certificate authority {route server} to verify the signature public key.

Hillier et al. discloses this in column 1, lines 45 through 65. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to employ a route server to create digital signatures of the authentication server's and product management server's public keys disclosed by Sprong et al. and Hicks et al. and validate these digital signatures by using the public key of the route server. One would have been motivated to do so in order to further prevent tampering or any other malicious activity.

Sprong et al. further discloses comparing the identification code and terminal code, which is located in an activation code, to a predetermined identification code and terminal code; and exiting the software release process if they are not equal, or alternatively continuing the process if they are determined to be equal (*ie. generating a serial number, wherein the serial number contains serial numbers of various hardware components on the host computer...checks if the serial number has been modified and either disabling the software or continuing the authorization process*) [column 10, lines 1-25].

**Claim 8:** Sprong et al., Hicks et al. and Hillier et al. disclose a license management method as in claim 7 above and Sprong et al. further discloses that the route public key is stored in the

Art Unit: 2135

software and the third determination step obtains the route public key from the software(*ie. unique identification number is assigned and recorded on the software, step 2*) [figure 1].

**Claim 9:** Sprong et al., Hicks et al. and Hillier et al. disclose a license management method as in claim 7 above and Sprong et al. further discloses that the authentication server has a software expiration date indicating an expiration date of the software(*duration and extend of authorized use*), wherein, in said fourth digital signature creation step, a digital signature of said terminal is created from the identification code, the terminal code, and the software expiration date using the private key of said authentication server, wherein, in said fourth checking step, said user terminal checks validity of the fourth digital signature using the public key of said authentication server obtained from said authentication server and obtains the identification code, the terminal code, and the software expiration date, and wherein, in said limitation release step, the functional limitation of the installed software is released [column 9, lines 46-57], but does not explicitly disclose that the limitation release step is based on the software expiration date verified as valid in said fourth checking step.

However, it would have been obvious to one of ordinary skill in the art at the time of invention to have the user terminal verify the expiration date of the software to be valid before releasing the functional limitation of the software. One would have been motivated to do so in order to prevent unauthorized users from using their software after the license has expired.

### ***Response to Arguments***

9. Applicant's arguments filed on June 29<sup>th</sup>, 2007 have been fully considered but they are not persuasive.

a. Regarding Claim 7, the Applicant argues that, "Specifically, one feature of the present invention resides in using the terminal code (corresponding to the MAC address in the description) fixedly allocated to the use terminal (25) and unique thereto. According to the present invention, supposing a case in which an old user terminal is replaced with a new user terminal, and thus software installed in the old user terminal must be installed in the new user terminal and activated, activation is permitted for a terminal code which is equal to or less than a number predetermined for each license code."

However, the Examiner respectfully disagrees and submits that this feature, in light of the new 35 USC § 112 rejections discussed above, is in fact disclosed by Sprong et al. in column 10, lines 1-25. Sprong et al. discloses comparing a serial number of a hardware component on a user's terminal, and if it is equal to a stored(predetermined) serial number, the activation is permitted, whereas if it is not equal the activation is not permitted.

b. Regarding Claim 7, the Applicant further argues that, "Independent claim 7 also recites a "releasing step [S48, S49], by the user terminal [5], of determining whether the identification code and the terminal code in the activation code correspond to the identification code and the terminal code transmitted at the first transmitting step, releasing the function limitation of the software when these codes correspond, and terminating the process of releasing the function limitation of the software when these codes do not correspond."

However, the Examiner respectfully disagrees and submits that Sprong et al. does in fact disclose this feature. Sprong et al. discloses comparing the identification code and terminal code, which is located in an activation code, to a predetermined identification code and terminal code; and exiting the software release process if they are not equal, or alternatively continuing

Art Unit: 2135

the activation process and activating the software if they are determined to be equal(*ie. generating a serial number, wherein the serial number contains serial numbers of various hardware components on the host computer...checks if the serial number has been modified and either disabling the software or continuing the authorization process*) [column 10, lines 1-25].

### ***Conclusion***

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

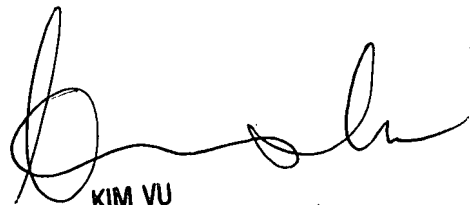
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Edward Zee whose telephone number is (571) 270-1686. The examiner can normally be reached on Monday through Thursday 9:00AM-5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

EZ  
September 17, 2007



KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100